UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 08-CR-10224-DPW
CHRISTOPHER SCOTT,	)	
	)	
Defendant.	)	

GOVERNMENT'S SENTENCING MEMORANDUM

Sentencing Recommendation

The seriousness of Christopher Scott's offense, his active partnership in an identity theft organization responsible for victimizing millions of people, and the profound need for general deterrence and punishment which reflects the seriousness of highly damaging computer network attacks, dictate the government's recommendation of 13 years' incarceration in this case.

The Nature and Scope of Scott's Criminal Conduct

The Gonzalez organization, of which Scott was a part:

1. Hacked into numerous businesses' wireless computer networks and databases;
2. Unlawfully accessed the computer networks that processed credit and debit card transactions for BJ's Wholesale Club, DSW, OfficeMax, Sports Authority and TJX Companies, among other companies;
3. Stole from the networks the data encoded on the magnetic stripes on the backs of credit and debit cards read by ATM machines and credit card readers pertaining to tens of millions of credit and debit card transactions;
4. Enlisted a person in a former Soviet Republic to decrypt encoded PIN

numbers;

5. Sold data in the United States and Eastern Europe for fraudulent use;

6. Used other data directly to withdraw large sums from bank's ATM machines; and

7. Used sophisticated techniques to launder their proceeds through surrogates, anonymous web currencies, and Latvian bank accounts in the names of shell corporations.[1]

Scott was Gonzalez's junior partner within the organization. It was Scott who, alone or sometimes accompanied by Gonzalez or his other friend, J. J., located which national retailers' wireless networks along Route 1 in Miami, Florida were vulnerable. *See*, *e.g.*, Presentence Report ("PSR"), ¶10 (pertaining to B.J.'s Wholesale Club). It was again Scott who, with the assistance of Gonzalez or J. J., exploited those vulnerabilities to systematically attack and explore the national retailers' computer networks. PSR, ¶¶10-12, 14-17. To do this, he probed the wireless networks of local stores for unsecured or insufficiently encrypted access points, broke in, and then bootstrapped that entry to access the networks where the national companies processed and stored customers' credit and debit card numbers and PIN numbers. *Id*. Finally, it was Scott who spent hour upon hour stealing tens of millions of credit and debit from the victim retailers. PSR, ¶¶10, 11, 14.

Scott hacked into and stole payment card databases from DSW, BJ's Wholesale Club, TJX Companies and other national retailers. DSW reliably estimated that Scott stole from their

[1] Gonzalez separately was involved with two Russian collaborators in a conspiracy to steal credit and debit card numbers by exploiting vulnerabilities in the corporations' databases, rather than their wireless networks. Scott was not involved in those activities.

systems more than 1,000,000 payment card numbers and TJX reliably estimated that Scott stole more than 11,000,000 current payment card numbers from theirs.[2] Each payment card number belonged to an individual victim.

The losses linked directly to Scott's wireless intrusions and data thefts identified to date – in the hundreds of millions of dollars – are five to ten times as large as those caused by any individual ever convicted in this District other than his co-conspirator, Gonzalez, and among the largest nationwide. As a direct consequence of Scott's attacks on their computer networks and theft of customers' payment card numbers, companies, banks and insurers lost close to $200 million. Among the victims hurt the worst were DSW, which lost between $6.5 million and $9.5 million; BJ's Wholesale Club, which lost between $11 million and $13 million; and TJX, which lost more than $170 million.

Within the Gonzalez organization, Scott was a valued lieutenant, not the head. Scott, himself, did not have the connections to obtain some of the malicious software tools he used, to decrypt PINs or to convert the credit and debit card numbers he stole into cash. PSR, ¶¶ 11, 12, 16. For this, he had to rely almost completely upon his senior partner, Gonzalez. *Id*. Gonzalez paid Scott richly, approximately $300,000-500,000 over the course of their partnership.[3] PSR, ¶21.

Basis of the Government's Sentencing Recommendation

---

[2] Outside counsel for both DSW and TJX retained expert consultants to conduct extensive forensic analyses of the intrusions and data thefts.

[3] Scott originally told investigators on May 7, 2008, that he made $400,000-$500,000 working with Gonzalez. He subsequently reduced that estimate to $300,000-$400,000. The $300,000-$500,000 approximation encompasses both these ranges.

The Advisory Sentencing Guideline Sentence

The Government's recommendation of 13 years imprisonment is significantly below the guideline range of life imprisonment. The guideline range is so high – corresponding to an offense level 45 – because the scheme victimized millions of people, targeted their identities, caused hundreds of millions of dollars in damages, and required Scott's special skills and the use of highly sophisticated techniques in order to succeed.

The Court should not sentence Scott below 13 years. From the outset, the plea agreement gave him a substantial sentencing benefit. In the face of a guideline range advising life imprisonment, the plea agreement permitted Scott to reduce his sentencing exposure by limiting the charges against him and capping his maximum sentence at twenty-two years.

The Critical Need for General Deterrence

The case before this Court will be a benchmark for other computer hackers and identity thieves, and there is no shortage of them out there. As Scott and Gonzalez demonstrated, Internet-based attacks require little capital investment and are highly profitable. To obtain victims' debit and credit card numbers thieves no longer need to dive into filthy restaurant dumpsters late at night to dig for carbon copies of diners' charge receipts. They can, with a well-executed attack like Scott and Gonzalez's, steal millions of payment card numbers from an insufficiently protected computer network while sitting in an apartment with a laptop and wireless card.

As a matter of general deterrence, this Court should clearly establish that the more extensive the harm which you knowingly and wilfully cause, the more you will be punished, even where your weapon of choice is a laptop keyboard. There has never been a computer

hacking and identity theft case prosecuted by the federal government where the financial cost has been so dear or the breadth of the personal victimization so large.

The Exceptional Seriousness of Scott's Offense

Christopher Scott was not a teenage misfit on a foolish frolic. For four years, Scott consciously, wilfully and purposefully broke into a dozen national retail computer networks. He took tens of millions of credit and debit card numbers, knowing that each belonged to someone whose account could be emptied of thousands of dollars if Gonzalez could sell the account number. And he intended that Gonzalez sell as many of those payment card numbers as possible. Committing large scale computer breaches and data thefts was an excellent job; it paid very well, provided him a comfortable living, and enabled him to buy a car, jewelry, and a nice house.

Proportional Punishment and Deterrence

Comparing the sentences that the government is recommending for Scott to others imposed for similar offenses is made challenging by the disparity in scale between Scott's crimes and previous computer crimes and identity thefts inside and outside the district. But the sentences in three significantly smaller but similar cases demonstrate why a sentence of 13 years' imprisonment for Scott is proportional and appropriate.

- Brian Salcedo. A much smaller and less successful version of Scott's scheme, Salcedo, also with Gonzalez's support, successfully compromised the Lowes computer network through a vulnerable wireless access point. Salcedo had stolen only a nominal amount of customers' credit card information when he was caught. Salcedo was sentenced to nine years' imprisonment in case no. 03-CR-53 in the Western District of North Carolina.

- Mario Simbaqueba Bonilla. Bonilla committed a series of computer intrusions, identity thefts, and credit card frauds. Bonilla, however, victimized only a tiny fraction of the number of people and caused only a small fraction of the harm Scott did – victimizing approximately 600 people and causing an attempted or actual loss of less than $1.5 million. Unlike Scott, Bonilla was active in the fraud as well as the computer intrusions and identity thefts. Bonillo similarly was sentenced to nine years' imprisonment in case number 07-CR-20897 in the Southern District of Florida.
- Max Ray Butler. Butler hacked into financial institutions, credit card processing centers and other secure computers in order to steal credit card account and other personal identification information which he then sold over the Internet and provided to an accomplice to use fraudulently. The victimization and loss inflicted by Butler were greater than that of Salcedo and Bonillo but still significantly less than that inflicted by Scott. Butler's computers contained approximately 1.8 million payment card numbers while the parties stipulated to a loss for guidelines purposes resulting from the scheme of $86.4 million. The government, as it is doing with Scott, filed a motion under U.S.S.G. § 5K1.1 on behalf of Butler in light of cooperation he provided following his arrest. Butler was sentenced to thirteen years' imprisonment in case No. 07-CR-332 in the Western District of Pennsylvania.

The only individuals in Gonzalez's organization who have been sentenced to date are Humza Zaman (09-CR-10054-MLW) and Stephen Watt (08-CR-10318-NG), neither of whom were principals and neither of whom provided substantial assistance.[4] Zaman, who did not

[4] Albert Gonzalez and Jeremy Jethro will be sentenced between the filing of this Memorandum and Scott's sentencing. Gonzalez and the government have entered into a binding

participate in any of the computer intrusions or identity thefts and was paid approximately $75,000 by Gonzalez to assist him in bringing about $700,000 back into the country, was sentenced to a guidelines sentence of 46 months' imprisonment by Judge Wolf. Watt who, according to both Gonzalez and Watt, edited the sniffer program used by Gonzalez in TJX, but was never told of its intended use, and did not participate in any of the other charged data thefts or profit in any way, was sentenced to two years' imprisonment by Judge Gertner.[5] Gonzalez's other principal lieutenant, Patrick Toey, has not been sentenced yet.[6]

Proportional treatment of defendants nationally is a core objective of federal sentencing. *See* 18 U.S.C. §3553 (a)(6); *United States v. Milo*, 506 F.3d 71, 76 (1st Cir 2007), *United States v. Ahrendt*, 560 F. 3d 69, 77 (1st Cir. 2009) ("[S]ection 3553(a)(6) aims primarily at the minimization of disparities among defendants nationally," quoting *United States v. Martin*, 520 F. 3d 87, 94 (1st Cir. 2008)). Brian Salcedo, Mario Simbaqueba Bonilla and Max Ray Butler all committed crimes similar in nature to that for which Scott presently is being sentenced. Because Scott's crimes are so much larger than theirs in size and were far more pernicious, a 13-year sentence for Scott would further 18 U.S.C. § 3553(a)'s goal of proportionate sentencing.

---

plea pursuant to Fed. R. Crim. P. 11(c)(1)(C). If accepted by the court, he will be sentenced to between 15 and 25 years' imprisonment for the crimes he committed with Scott. The government has argued in its Sentencing Memorandum in Gonzalez's case that Gonzalez should be sentenced to 25 years' imprisonment. Jethro sold malicious software to Gonzalez, but had no involvement in either Scott's network intrusions and payment card thefts, or Gonzalez's subsequent sale of the payment cards and laundering of the sales' proceeds.

[5] While the government agrees that Watt was less culpable than Gonzalez, Christopher Scott and Patrick Toey, the government respectfully disagrees with Judge Gertner's finding that Watt was "less culpable than all the other participants" and strongly disagrees with the sentence she imposed.

[6] Patrick Toey is scheduled for sentencing before Judge Young on April 15th.

Scott's Assistance in the Investigation and Prosecution of This Matter

The government's sentencing recommendation for Scott reflects both his relative role in the Gonzalez organization[7] and his assistance in the investigation of this matter. That assistance was useful but limited.

Gonzalez compartmentalized the information he shared with his collaborators, making Scott a useful historian of the wireless intrusions and data thefts, and enabling him to identify some (of his own) corporate victims previously unknown to the government. Scott's information expanded investigators' understanding of the case. Albert Gonzalez knew, had he proceeded to trial, that Scott would have provided both valuable corroboration of co-conspirator Patrick Toey's testimony and explanatory background for the extensive forensic and documentary evidence developed independently in the investigation.

However, by the time Scott agreed to cooperate with the government, Patrick Toey already had been debriefed over the course of two weeks about the activities of the Gonzalez organization (including Scott), and had provided full access not only to his own computer but also to the Latvian and Ukrainian servers used by Gonzalez.[8] Further, initially Scott was not fully forthcoming with law enforcement agents, potentially damaging his credibility if required to testify at trial.

---

[7] Scott's relative role in the organization is described at pp. 1-2, above.

[8] A reflection of his good tradecraft, Gonzalez used hard-to-locate and easily abandoned offshore and compromised computer servers to facilitate his collaborators' work. The Latvian and the Ukrainian computer servers were the last in the series and were established after the wireless intrusions and data thefts perpetrated by Scott. Among other purposes to which they were put, the Latvian and Ukrainian servers stored stolen payment card numbers (including some of those stolen by Scott) and malicious software (including a variant of the sniffer program used by Scott to steal payment cards being processed by TJX). Gonzalez provided other computer servers for Scott to use, as necessary.

Scott already has benefitted from his assistance in the investigation of the Gonzalez organization in a separate case. Following the search of his house for evidence of the computer intrusions, Scott was charged with the possession of a firearm in furtherance of a drug offense in the Southern District of Florida. (He had a marijuana grow lab in his house protected by numerous firearms). The Florida case, number 08-20718 in the Southern District of Florida**,** was transferred here for plea and sentencing before Judge Tauro and assigned case number 08-CR10240-JLT. In light of the assistance provided by Scott, the government is filing a motion under 18 U.S.C. § 3553(e) in that case and is recommending that Judge Tauro impose a sentence below the otherwise applicable mandatory minimum.

Neither Attention Deficit Disorder Nor Self-Medication with Marijuana, if Accurate Diagnoses, Justifies or Diminishes Scott's Criminal Conduct

When interviewed by Probation for the Presentence Report, "the defendant describe(d) his mental health as 'good,' noting that prior to November 2008, he had never met with, nor felt the need to meet with, a mental health counselor." Presentence Report ("PSR"), ¶83. In contrast, just prior to this sentencing, Scott's counsel retained a forensic psychologist who opined that Scott met the "diagnostic criteria for several mental disorders." Appendix A, Report of Michael P. Brannon ("Brannon Report") at 5. These included: Panic Disorder NOS, Depressive Disorder NOS, Attention-Deficit/Hyperactivity Disorder, Cannabis Dependence Disorder, Alcohol Abuse and Personality Disorder NOS (with avoidant and obsessive traits). *Id.* The examiner concluded that the criminal conduct to which Scott has pled guilty "appear(s) consistent with the impulsivity, impaired judgment and poor anticipation of future consequences often observed with these conditions."

To the extent that the last-minute report of psychologist Michael Brannon is being

offered by the defendant as an explanation or justification for his criminal conduct, it should be ignored. The psychologist did not review enough information about the case to support his conclusion that mental disorders caused Scott to commit an entire series of elaborate and massive computer intrusions and data thefts over the course of four long years. "The Sources of Information," found on page 1 of his report, notably do not include: (I) Probation's statement of facts in this case; (ii) a transcript of the course of conduct acknowledged by Scott at his Rule 11 hearing; or, most basically, (iii) the Information itself to which Scott pled guilty. Moreover, even if it were proven conclusively that Scott presently suffers from one or more of the *seven* disorders enumerated in Mr. Brannon's diagnosis,[9] this would neither explain nor justify Scott's persistent efforts over months and years to break into numerous major computer networks, probe the networks for payment card numbers and then patiently download millions of them for sale. There are quite literally millions of people in the United States with each of the generic disorders of which the forensic examiner believed he found evidence, none of whom make their living for four years hacking into networks and stealing credit and debit card numbers.

Scott was prompted by a common set of human motivations: companionship, challenge and greed. Dr. Brannon acknowledges the first two. Scott liked being part of the hacker community. And he liked the challenge that each network intrusion presented him. Brannon Report at 3. But above all, Scott liked the fact that stealing victims' credit and debit cards and selling them for as much as he could generated several times as much money as he could earn legitimately. At first, this enabled Scott to rent limos and go clubbing with up to ten women at a

[9] There is no question that Scott smoked marijuana, a matter explicitly excluded as a matter of consideration in sentencing under the advisory Sentencing Guidelines. *U.S.S.G. § 5K2.13*.

time, by his own account. Later, it enabled him to buy a car and a $400,000 home for his girlfriend and family. *See* PSR, ¶¶108-110.

Scott's Challenges to Probation's Guidelines Calculations are Meritless

Scott makes three core challenges to the guideline calculations made by Probation in the initial PSR. First, he argues that he, personally, did nothing sophisticated when exploiting corporate networks and, accordingly, §2B1.1(b)(9)(C) is inapplicable. Second, he asserts that three guideline enhancements should not be applied simultaneously because they are identical: U.S.S.G. §§2B1.1(b)(9)(C) (offense involved sophisticated means), 2B1.1(b)(10) (offense involved trafficking in unauthorized access devices) and 3B1.3 (defendant used a special skill to significantly facilitate the offense). Lastly, he contends that Probation's loss calculation is exaggerated and insupportable. While none of these challenges detracts from the enormity of the harm which Scott caused or his level of commitment to wireless data thefts more than four years, they are addressed in order, below.

Scott's Efforts Were Sophisticated

Scott repeatedly points to what other conspirators did, without ever fully acknowledging what he, himself, did. In this instance, he suggests that because he did not use SQL injection attacks to access corporate networks as Patrick Toey did, somehow, by definition, his own efforts were not sophisticated. The wireless intrusions and data thefts in which Scott played a role were highly sophisticated: (I) accessing vulnerabilities of wireless networks; (ii) compromising encryption protocols; (iii) locating within complex corporate networks sensitive payment data; (iv) stealing that data without leaving compromising traces; (v) installing a VPN connection between TJX's financial processing servers and a server which Gonzalez obtained for Scott, and (vi) utilizing sniffer programs to capture password/account information and current

unencrypted payment card data. PSR, ¶¶10, 12-16. All of these activities were sophisticated, every bit as much so as Patrick Toey's later SQL injection attacks.

U.S.S.G. §§2B1.1(b)(9)(C), 2B1.1(b)(10) and 3B1.3 are Not Identical

Scott's argument that U.S.S.G. §§2B1.1(b)(9)(C), 2B1.1(b)(10) and 3B1.3 address the same single characteristic and should not be separately applied is without merit. U.S.S.G. §2B1.1(b)(9)(C) - - sophisticated means - - addresses whether the crime was sophisticated, whereas U.S.S.G. §3B1.3 - - special skills - - addresses whether the defendant used special skills in the commission of that crime. For example, had Scott simply "cashed out" at ATMs payment card numbers stolen from computer networks victimized by Gonzalez, while the crime in which Scott and Gonzalez were engaged still would have involved the use of "sophisticated means," Scott himself would not have used any special skills in its perpetration. Moreover, one can traffick in unauthorized access devices in unsophisticated ways and without the use of computer skills. Credit cards and debit cards are routinely stolen from wallets and simply resold on the street or used to make fraudulent purchases. *See, e.g.*, *United States v. Savarese,* Criminal No. 07-10320-RGS (D. Mass. Filed Sept. 26, 2007).

The Scope of the Harm Caused by Scott's Computer Intrusions and Payment Card Thefts is Well Established

The impacts of Scott's intrusions and payment card number thefts were sufficiently great that TJX, BJ's Wholesale Club, DSW, and OfficeMax were all required to report them in filings with the Securities and Exchange Commission. Accordingly, the corporate victims were required to determine and report their losses in accordance with generally accepted accounting standards. Further, when submitting their filings to the SEC, each of these established corporations, their principals and their counsel were doubtless aware that misleading statements

could be met with severe civil and criminal penalties. *See, e.g.*, 18 U.S.C. §1350 (requiring chief executive officers and chief financial officer to submit statements with each periodic SEC report affirming the accuracy of the reports).

TJX has filed a victim impact statement, representing to the Court those losses directly attributable to the Scott and Gonzalez's intrusion into, and massive identity theft from, its computer networks. The victim impact statement enables the Court to separate those losses already incurred from those that are likely but that TJX has not yet incurred. The Victim Impact Statement also refutes the defendant's claim that his criminal conduct did not cause all of the losses suffered by TJX's shareholders and formally reported to the SEC:

> As required by and consistent with applicable accounting standards, TJX has estimated its total cost related to the Computer Intrusion in its quarterly and annual financial statements filed with the Securities and Exchange Commission. As of October 31, 2009, TJX estimated those costs as $171.5 million, at which date $146.3 million had been expended and $25.2 million had not yet been spent but was reasonably probable and estimable.
>
> * * *
>
> The total costs reflect only cash costs resulting directly from the Computer Intrusion that were incremental to costs TJX would otherwise have incurred. The total costs do not reflect the very substantial costs of TJX's own personnel in dealing with the Computer Intrusion. The total costs are net of insurance recoveries received by TJX.

Victim Impact Statement of TJX Companies, Inc., pp. 3-4.[10]

---

[10] A victim's conduct, while not affecting the loss for the purposes of determining a defendant's specific offense characteristic from the Guidelines' loss table, indeed may be a basis for a departure if the loss calculation overstates the seriousness of the offense. *United States v. Maldonado-Montalvo*, 356 F.3d 65, 69 (1st Cir. 2003). "Theoretically, such a loss overstatement may occur where, *inter alia*, '[a]ny portion of the total loss sustained by the victim [is] is a consequence of factors *extraneous to the defendant's conduct*.'" *Id.* at 69 (quoting *United States v. Reeder*, 170 F.3d 93, 109 (1st Cir. 1999))(citations omitted, emphasis in the original). However, here, no extraneous factors increased the number of credit and debit cards which Scott stole and continued to "cash out" or sell. Similarly, no extraneous factors amplified how

Scott's challenge to the accuracy of the number of payment cards which he stole similarly fails.[11] From the outset, Scott should not be able to benefit from the fact that he used intrusion and data theft techniques designed to conceal his presence and thefts from his victims. Notwithstanding his use of such techniques, however, both DSW and TJX were able to reliably determine that Scott stole a minimum of one million and 11.2 million current, unexpired payment cards from their respective computer networks through extensive forensic analyses by outside experts. Further, TJX, again subject to severe criminal and civil penalties, reported the number stolen from their network in its SEC filings.[12]

Conclusion

Christopher Scott and Albert Gonzalez, assisted to a lesser extent from time to time by J.J., systematically broke into the computer networks of numerous national retailers and stole millions of victims' credit and debit card numbers for fraudulent use. Unquestionably, Gonzalez was the leader of the enterprise: he had the connections to obtain malicious software tools which Scott methodically used, to decrypt PIN numbers associated with payment cards Scott stole, and

---

extensively issuing banks and credit card companies reacted, the number of innocent cardholders affected, the resulting losses which had to be borne by them or passed back to victim retailers and the potentially devastating harms to retailers' businesses caused by the publicity surrounding Scott's massive break-ins and payment card thefts.

[11] Indeed, the argument is questionable since Scott himself stated during debriefings following execution of his proffer and plea agreements that he took as many as or more payment cards from DSW and TJX than forensic analysts retained by the victims were able to identify.

[12] Among Scott's most profitable network intrusions and payment card thefts was OfficeMax. In a logged chat session with co-conspirator and payment card fence, Maksym Yastremskiy, Gonzalez reported that 11 million card numbers were downloaded from OfficeMax in 2003-2004, and that Gonzalez had been able to decrypt almost one million before they expired. These additional card numbers are not being relied on for sentencing purposes so that it is not necessary for the Court to resolve the reliability of Albert Gonzalez's statements.

to sell the millions of numbers Scott stole. Equally unquestionably, though, Scott was integral to Gonzalez's success. Scott persistently sought out national retailers using wireless networks which were either unencrypted or poorly encrypted, then probed those networks for weaknesses he could exploit and harvest victims' payment card numbers. Absent a measure for Scott's limited assistance to the government, Scott should receive a sentence below that imposed on Gonzalez in light of their relative roles, but not dramatically so. The two were partners in the wireless intrusions and payment card number thefts; had either of them not so willingly participated, corporate victims would have been spared nearly $200 million in losses and tens of millions of cards – each of which belonged to a victim – would not have been stolen for sale and fraudulent use.

Scott's obsession with computers, feeling of comradery with friends in the hacking community, attention deficit disorder (if he has it), and use of marijuana, cannot, and should not, justify the extraordinary crimes he committed over the four-year span of 2003-2007, or diminish the responsibility he should bear for committing them. Scott deserves a significant sentence for the previously unparalleled harm and victimization he knowingly and willfully caused. The community of hackers and data thieves of which Scott was proud to belong is too large and growing; it is important that Scott's sentence send a strong deterrent message to them.

For the reasons detailed above, Scott should be sentenced to:

(a) 13 years' imprisonment,

(b) three years' supervised release, a condition of which is that he not be permitted any unmonitored use of an internet accessible device absent prior approval of probation and that any employer giving him access to computer equipment be previously informed of his conviction in this case,

(c) no fine, in light of the amount of restitution owed,

(d) restitution in the amount of $189 million, and

(e) a special assessment of $400.

Respectfully submitted,

CARMEN M. ORTIZ
United States Attorney

By: */s/ Stephen P. Heymann*
STEPHEN P. HEYMANN
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann
STEPHEN P. HEYMANN
Assistant U. S. Attorney

Date: March 21, 2010